Exhibit B

The F5 Handbook for Service Providers

24 Use Cases to Secure, Optimize, and Monetize Your Network

Table of Contents

Optimize, Secure, and Monetize Your Network

Mobile consumers are growing accustomed to anytime/anywhere access from their mobile devices to resource-intensive content, such as streaming video and high-bandwidth applications. Mass-market consumption of smartphones and other connected mobile devices, along with advanced 4G LTE network deployments, have led to massive and sustained growth in data usage. As a result, operating costs are rising while average revenue per user (ARPU) has trended flat to negative. To remain profitable, service providers must find new ways to support increased demands on their networks with more efficient resource utilization, while maintaining the ability to support rapid rollout of new revenue-generating services.

F5 offers solutions for fixed and mobile service providers to achieve maximum optimization, security, and monetization of their networks. The sections below feature use cases that illustrate how you can maintain top network performance and profitability.

SECURITY SOLUTIONS

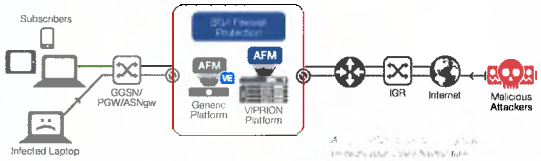
S/Gi Firewall

THE CHALLENGE

As mobile network operators and other service providers migrate to all-IP based networks such as 4G LTE, network intrusions and attacks are far more likely to occur. Service providers must constantly defend against security threats to ensure the availability of their most precious resource—the network. This increases costs and operational complexity, and has a negative effect on network performance and the subscriber experience.

F5 HELPS YOU:

- Protect the core infrastructure with a high performance, highly scalable
- Defend against DDoS attacks across all layers



THE SOLUTION

F5® BIG-IP® Advanced Firewall Manager™ (AFM) defends the mobility infrastructure and mobile subscribers from attacks, regardless of their source. This capability includes mitigation of large-scale DDoS attacks such as network floods, port scans and sweeps, or connection floods. By detecting and stopping these types of attacks, BIG-IP AFM can prevent congestion and overloading of the control and bearer planes of the radio access network. BIG-IP AFM protection against DDoS attack vectors continues to increase with each version released. With many BIG-IP platforms, DDoS protection functions are accelerated using specialized hardware.

BIG-IP AFM, as an ICSA Labs Certified firewall solution, offers true protection of a full-proxy firewall, meaning that it fully terminates and inspects incoming client connections for threats. You'll have the assurance of network availability and an improved subscriber experience.

SECURITY SOLUTIONS

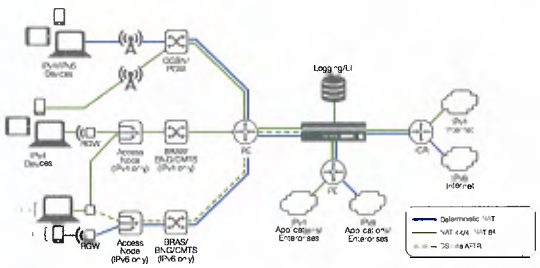
Carrier-Grade NAT

THE CHALLENGE

The worldwide proliferation of wireless and Internet-enabled devices has rapidly depleted IPv4 addresses, and by 2018, 40 percent of mobile data traffic will be IPv6 addressed. Service providers are being challenged to support and manage existing IPv4 devices and content in the network, while at the same time transitioning to support newer IPv6 devices and applications. And because IPv6 devices and content are not backward compatible with IPv4, any IPv6 migration strategy needs to support the coexistence of IPv4 and IPv6 during the transition.

F5 HELPS YOU:

- Migrate to IPv6 and IPv6 with flexible deployment options
- Optimize network performance with carrier-grade performance and scalability
- Reduce server quantities and management costs



THE SOLUTION

F5 BIG-IP® Carrier-Grade NAT (CGNAT) offers a broad set of high-performance, highly scalable tools that enable service providers to successfully migrate to IPv6 while continuing to support and interoperate with IPv4 devices and content. In addition, BIG-IP CGNAT provides extensive, flexible high-speed logging capabilities along with support for IPFIX, which compresses NAT logging, therefore reducing the amount of data per log entry and minimizing overall costs.

BIG-IP CGNAT offers tunneling solutions, including Dual-Stack Lite (DS Lite) capabilities that allow you to support legacy IPv4 endpoints in your IPv6 network. DS Lite capabilities consist of endpoint IPv4 packets being encapsulated in an IPv6 tunnel and sent to an external IPv4 destination through your network. In addition, IPv6 rapid deployment (6rd)—another tunneling service— enables networks on IPv4 to communicate with IPv6 addresses without upgrading hardware.

BIG-IP CGNAT also provides network address translation (NAT) functionality, enabling you to continue delivering IPv4 connectivity and to handle high numbers of concurrent sessions as you manage IPv4 address depletion and plan for a seamless migration to IPv6. F5 NAT functionality includes NAT44, which allows you to primarily focus on extending the use of IPv4 addresses in your network, as well as NAT64, which enables IPv6 endpoints to seamlessly and transparently access IPv4 content and destinations. BIG-IP CGNAT also supports 464XLAT and DNS64, which uses DNS AAAA records so IPv6 hosts can see IPv4 destinations as IPv6 addresses.

SECURITY SOLUTIONS

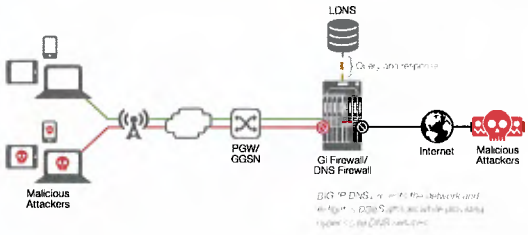
Intelligent DNS Firewall

THE CHALLENGE

Service providers use DNS to enable subscriber access to critical services and web applications. If DNS is unavailable, services will fail to function properly, leading to network and service degradation or failures. Service providers need to optimize and secure the DNS infrastructure to better serve mobile users. However, such an infrastructure requires a tremendous amount of real-time management and stability, and scaling DNS rapidly becomes critical when dealing with millions of service names and IP addresses. As service providers scale their control planes, they also need to ensure the security of subscriber and billing data, as well as the capacity to withstand attacks such as DNS DDoS attacks, DNS amplification attacks, and DNS tunneling for circumventing service limits.

F5 HELPS YOU:

- Optimize DNS infrastructure and hyper scale service delivery
- Monetize with improved network performance and lower churn
- Secure your network and mitigate DNS attacks and circumvention
- Ensure service experience and extend service availability



THE SOLUTION

F5 BIG-IP® DNS makes it easy for service providers to optimize, secure, and monetize their DNS infrastructures. The solution provides carrier-grade, high-performance LDNS caching and resolving, and is a hyper-scale authoritative DNS solution that includes DNS firewall security services for mitigating DNS DDoS attacks. BIG-IP DNS delivers an intelligent and scalable DNS infrastructure for faster access and service response for mobile users. In addition, it can load balance local and recursive DNS services. Service providers use customizable monitors and GSLB services to allocate the best resources to DNS queries and respond with the best service experience. BIG-IP DNS also enables a DNS64 environment, creating a fault-tolerant architecture—optimizing network traffic and increasing QoE for users, thus protecting service providers' brand.

In addition, BIG-IP DNS shields the DNS infrastructure from malicious attacks via infected subscribers and from undesired DNS queries and responses that reduce DNS and service performance. This intelligent DNS firewall from F5 inspects and validates protocols while dropping invalid requests or refusing to accept unsolicited responses. BIG-IP DNS is an ICSA Labs Certified network firewall with DDoS threshold alerting that hyper-scales across many devices using IP Anycast for DDoS absorption. It mitigates threats by blocking access to malicious IP domains.

Finally, BIG-IP DNS offers enhanced, detailed stats with high-speed DNS logging and reporting, along with advanced analytics and performance metrics to deliver business intelligence for service and capacity planning, service optimization, and service monetization, as well as security troubleshooting.

SECURITY SOLUTIONS

VoLTE and IMS Security

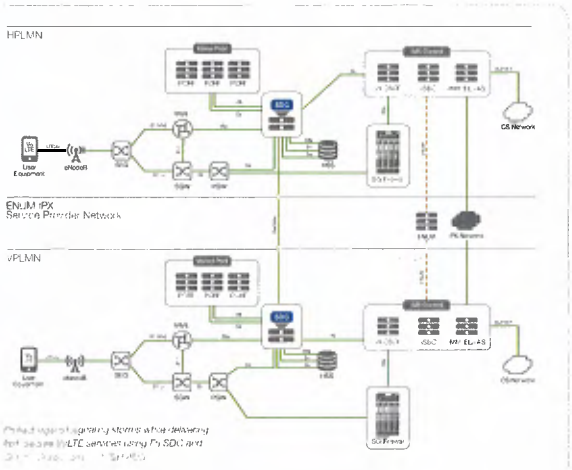
THE CHALLENGE

VoLTE [illegible] circuit switch networks to all-IP LTE networks in order to reduce overall network operation costs. The rate of VoLTE adoption is rapidly increasing (including one North American T-1 operator with nearly 40 percent of its voice calls on VoLTE). As VoLTE matures, attacks against the signaling resources used to provide services to customers—including real-time signaling protocols—will also increase. As a result, VoLTE security—focusing on protecting and controlling signaling protocols including Diameter and SIP, for example—is becoming more critical.

Additionally, with more and more devices coming to the market with support only for IPv6, the ability to manage and control potential signaling spikes caused by these IPv6 devices is equally important. When a SIP signaling storm occurs due to unintended actions, other node outages in the network, or malicious attacks, it is important to rate-limit SIP requests to the P-CSCF so that it is not overwhelmed. Plus, [illegible] the types and numbers of new devices also come massive [illegible], with [illegible] changes, operators will require solutions capable of very high connection rates and increasing concurrency.

F5 HELPS YOU:

- Deliver fast and secure VoLTE service
- Provide the highest possible security protection
- Support high connection rates and a high level of concurrency
- Protect the brand and maximize subscriber QoE



[illegible] signaling storms while delivering [illegible] LTE services using F5 SDC and [illegible]

THE SOLUTION

F5 helps service providers deliver fast and secure VoLTE services. The F5 Traffix™ Signaling Delivery Controller™ (SDC) and BIG-IP platform with SIP application layer gateway (ALG) capabilities help ensure VoLTE service continuity and protect against unauthorized access, unexpected traffic peaks, signaling storms, session spoofing, and privacy attacks. The F5 firewall solution with SIP ALG monitors SIP messages and only permits RTP streams when the SIP ALG validates the SIP control channel and thus can provide security for user traffic in the network. By combining firewall, traffic management, DDOS protection, and carrier-grade network address translation (CGNAT) functions on the S/Gi LAN with SDC signaling control directly in front of the P-CSCF, F5 solutions can secure and distribute traffic, regardless of whether that traffic is from IPv4 or IPv6 services. By doing so, the F5 solutions combine security and availability functionalities to maintain network service during times of unexpected stress.

Additionally, F5 solutions enable service delivery with the highest possible protection, connection rates, and concurrency levels in the industry—more than a terabit of throughput and up to 1.2 billion concurrent connections.

SECURITY SOLUTIONS

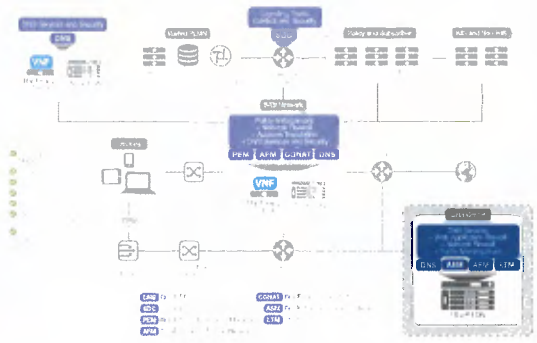
Data Center Firewall

THE CHALLENGE

Service providers' networks continue to grow to adopt 4G and 5G technologies, rapidly deploy new services based in the data center, and host applications such as video and content streaming. These changes not only threaten quality of service for users and increase capital and operational expenses, but also strain the security architecture's ability to handle a rapidly changing threat landscape. As a result, service providers need to enable growth while ensuring reliable and scalable security.

F5 HELPS YOU:

- Rapidly deploy new, revenue generating services and applications based in the data center
- Increase connection rates and concurrency
- Reduce space, power consumption, and TCO
- Improve quality of service for users



F5 solutions deliver comprehensive network protection from the data center to DNS infrastructures

THE SOLUTION

F5 delivers a full range of solutions that simplify service providers' security architectures while mitigating threats. The full proxy architecture of F5 solutions also allows service providers to attain extensive visibility and control throughout layers 4 through 7. This enables granular control of all connections, more extensive security functionality, and comprehensive end-to-end protection against DDoS and other attacks. F5 solutions protect targeted network elements, the DNS infrastructure, devices, and applications with features that include application health monitoring, a robust web application firewall, web access controls, TCP optimization, web acceleration, L7 DDoS protection, and broad SSL support including SSL inspection and offload.

A leading T-1 service provider that implemented F5 data center firewall solutions reduced its hardware footprint by a factor of 20—a big improvement for scalability. Typical data center footprints can be reduced even more dramatically with F5 solutions for securing DNS. Ultimately, these solutions help simplify operations and lower total cost of ownership while securing the network and protecting the service provider's business and brand.

DATA TRAFFIC MANAGEMENT SOLUTIONS

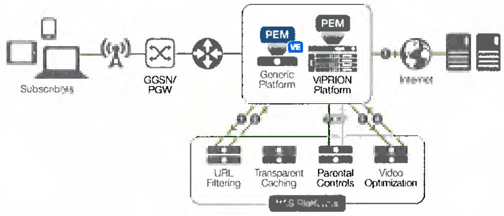
Dynamic Service Chaining/ Intelligent Traffic Steering

THE CHALLENGE

To support the growing number of services offered to subscribers, service providers have deployed multiple value-added service (VAS) platforms from a variety of different vendors. However, these platforms cause more network complexity, increased deployment and operating [illegible] All data traffic [illegible] to these platforms on [illegible] layer 3 and layer 4 equipment (including policy-based routers), regardless of relevance. As a result, all VAS [illegible]

F5 HELPS YOU:

- Reduce deployment and operation costs
- [illegible]
- Reduce [illegible]
- Increase ARPU [illegible] services
- [illegible]
- [illegible]



[illegible]

THE SOLUTION

F5 BIG-IP® Policy Enforcement Manager™ (PEM) provides subscriber- and context-aware traffic management with the ability to perform layer 7 advanced steering to multiple VAS platforms (including web caching, video optimization, and parental control) based on parameters such as subscriber profile, device, content type, location, and network conditions. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video optimization server. By steering traffic only to relevant servers, you can reduce the burden on other servers, thereby reducing CapEx and OpEx. Intelligent traffic steering can decrease the traffic to your VAS platforms by 50 to 75 percent, significantly saving CapEx and OpEx on VAS platforms and lowering total cost of ownership (TCO).

To add more value for subscribers, you can leverage the dynamic service-chaining capabilities of BIG-IP PEM to link multiple services together. Dynamic service chaining enables you to send traffic to multiple value-added services within a single flow. For instance, BIG-IP PEM can send subscribers who want to watch a specific video clip to a URL filtering/parental control service before sending it to a video optimization server, ensuring that these subscribers are allowed to view the content. With dynamic service chaining, you can create differentiated services and provide opportunities to increase ARPU.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Subscriber and Application Bandwidth Control

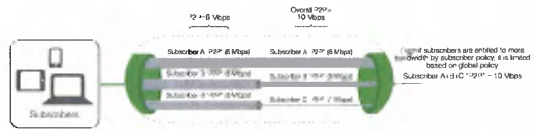
THE CHALLENGE

During peak times, heavily congested broadband networks can cause subscribers to have difficulty streaming both high-bandwidth video and low-bandwidth web applications. This causes a significant deterioration in subscriber QoE. As a service provider, your challenge is to deliver a high quality of service (QoS) to your subscribers at all times, even during periods of heavy network congestion.

F5 HELPS YOU:

- Optimize network performance
- Increase ARPU with new services
- Gain additional brand and subscriber loyalty and reduce churn

Global Application Control



Per-Subscriber Application Control

Bandwidth control limits can be applied at the application level, or at a per subscriber, per application level.

THE SOLUTION

BIG-IP PEM delivers insight into subscriber behavior and effectively manages network traffic with a wide range of policy enforcement capabilities, thereby optimizing network performance by implementing bandwidth control policies at the subscriber and application level.

As a subscriber-aware solution, BIG-IP PEM can identify subscriber usage and the type of plans they have implemented. Leveraging this information, BIG-IP PEM can provide subscriber bandwidth-controlling mechanisms via rate limiting, DSCP marking, and layer 2 QoS marking. These limits can be applied to a group of subscribers or to all subscribers, or even at the application level. With these limits, you can establish tiered services to create and manage incremental revenue-generating plans based on subscribers' actual data usage patterns. You can also use bandwidth control to implement fair-usage policies that allow subscribers to consume a fair amount of bandwidth while you distribute it more proportionally across the subscriber base.

Traffic classification is a key feature of BIG-IP PEM. This enables you to identify the types of applications, services, and protocols that are being used to help you create application-specific plans or rate limits. Control how much bandwidth is being allocated for specific applications, such as rate-limiting P2P applications, during peak network congestion levels. BIG-IP PEM classifies traffic into several categories of applications and protocols including P2P, VoIP, web, and streaming applications.

DATA TRAFFIC MANAGEMENT SOLUTIONS

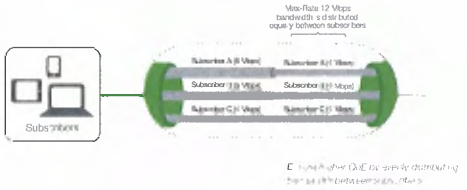
Fair Usage Policy

THE CHALLENGE

Service providers need to provide consistent QoE to ensure that subscribers receive the service they have signed up for. However, many networks have a small percentage of subscribers classified as heavy data users who continuously download and stream large amounts of [illegible] impacting the ability for other users who occasionally stream or download content from getting the bandwidth they have paid for.

F5 HELPS YOU:

- Decrease network congestion
- Provide high QoE to subscribers
- Reduce churn



THE SOLUTION

Leveraging BIG-IP PEM, you can detect heavy data users and the type of applications they are using. Subscriber and application awareness functionality helps you control rates on a per-subscriber and per-application basis, according to their existing rate plan. By evenly distributing bandwidth between subscribers and tightly allocating bandwidth, you'll ensure higher QoE while efficiently managing network resources.

DATA TRAFFIC MANAGEMENT SOLUTIONS

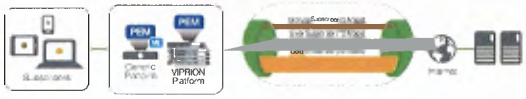
Tiered Service Plans

THE CHALLENGE

Service providers want new services that will help drive revenue while providing a high QoE to their subscribers. These service providers cater to diverse subscriber bases with different expectations in the amount of bandwidth they require and how much they are willing to pay.

F5 HELPS YOU:

- [illegible]
- [illegible]
- [illegible]



Offer rate plans based on subscriber preferences and their bandwidth requirements

THE SOLUTION

Tiered service plans let you offer specific rate plans based on subscriber preferences and their requirements for bandwidth and broadband speed. A certain market demographic may require the highest speeds possible while others only need content with best effort. The ability to offer tiered service plans with quota management ensures a high QoE for your subscriber base and increased revenues from those who utilize the network the most. For example, you can implement a bronze, silver, or gold plan. Bronze and silver subscribers would be capped at a certain data limit and best-effort data speeds, whereas gold subscribers would get unlimited data and guaranteed class of service. Service plans can also be [illegible]

DATA TRAFFIC MANAGEMENT SOLUTIONS

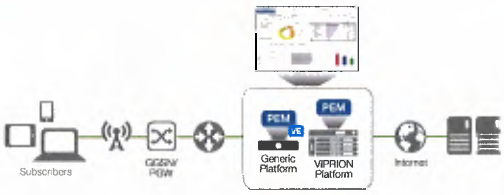
Analytics

THE CHALLENGE

New services allow service providers to cater more closely to subscriber needs and preferences. Until recently, however, service providers couldn't get detailed information on their subscribers' network usage or preferred applications. This lack of data meant that they could only offer "one size fits all" models of generic services and rate plans. But increased competition required service providers to rethink their approach. Solutions with application visibility now give them an opportunity to offer more innovative services.

F5 HELPS YOU:

- Introduce innovative new services
- Increase ARPU/brand loyalty



Analytics gives you new ways to provide and charge for services for your subscribers.

THE SOLUTION

BIG-IP PEM classifies traffic based on application type, giving you new ways to provide tailored services for your subscribers, generate new revenues, and increase customer satisfaction. With application charging and quota management, you can offer customized service plans based on subscriber requirements. For example, subscribers may be interested in a VoIP package. For an additional cost, you can offer a plan that will give those subscribers unlimited VoIP usage. If subscribers want a business package, you can offer the service-enabling business applications to be used without affecting those subscribers' data caps. Analytics lets you offer multiple types of services based on specific market demographics—resulting in increased revenues, improved user experience, and greater brand loyalty.

DATA TRAFFIC MANAGEMENT SOLUTIONS

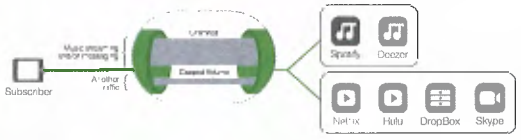
OTT Monetization

THE CHALLENGE

Over-the-top (OTT) providers put pressure on service providers by offering bandwidth-intensive applications that drive networks to full capacity, while providing minimal or no revenue to the service providers. As a service provider, you can become more proactive and develop joint partnerships with these OTT providers rather than let them take all the revenues.

F5 HELPS YOU:

- Achieve higher QoE for subscribers
- Increase revenues



Develop joint partnerships with OTT providers to offer services to your subscribers.

THE SOLUTION

With BIG-IP PEM, you can detect and classify specific applications and implement effective policies, such as providing a higher QoS to specific applications or exempting applications from a subscriber's data cap. For example, you can identify a video-streaming application and determine that a subscriber has paid for the premium package. The subscriber then receives guaranteed QoS at all times for that application, while other applications are delivered based on best effort. You can also identify specific OTT applications and exclude those from a subscriber's data usage. For instance, subscribers using Facebook would be zero-rated, whereas other applications would count against their data cap. In both scenarios, you can form business partnerships with OTT providers and be paid for these services.

DATA TRAFFIC MANAGEMENT SOLUTIONS

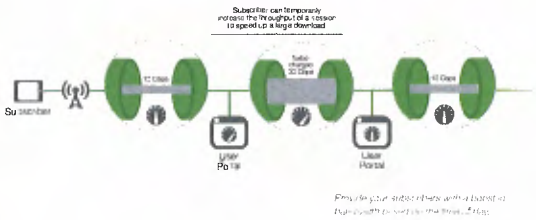
Bandwidth on Demand

THE CHALLENGE

Increased demand for bandwidth requires service providers to expand their networks and add capacity to accommodate subscribers. However, peak traffic only happens at certain times of the day. While other times, service providers may have ample capacity with network components sitting idle, resulting in potential lost revenue.

F5 HELPS YOU:

- Optimize network resources
- Provide higher subscriber QoE
- Increase revenue opportunities



THE SOLUTION

You can further differentiate your offerings by adapting to subscribers' real-time bandwidth requirements and quota management. A subscriber may only want a boost in bandwidth for a certain amount of time each day (either on- or off-peak hours). This gives you an opportunity to generate incremental revenue by charging a premium to the subscriber for that period. You can also monitor your network for low utilization during off-peak hours, letting subscribers opt in for an additional fee to get higher bandwidth speeds during these less-congested times. In both cases, once the time period is over, the subscriber will resume normal broadband speeds you'll generate additional revenue while more efficiently utilizing network resources.

DATA TRAFFIC MANAGEMENT SOLUTIONS

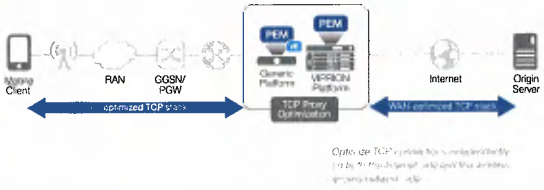
TCP Optimization

THE CHALLENGE

Within 3G/4G networks, mobile users are subject to the network connections based on the characteristics of the wireless access network—typically high latency, packet loss, and congestion. On the internet side, the network has different performance characteristics including low latency, low packet loss, high bandwidth, and minimal congestion. To ensure the best customer experience, service providers must implement a solution to optimize the connection on both the internet side and the wireless access network.

F5 HELPS YOU:

- Provide higher QoE to subscribers
- Increase revenues with increased data usage



THE SOLUTION

Leveraging the BIG-IP system, you can optimize the TCP connections independently on both the internet side and the wireless access network side. The result will be a significant performance boost for data transfer rates and up to a 200 percent bandwidth utilization improvement—significantly increasing QoE for your subscribers.

DATA TRAFFIC MANAGEMENT SOLUTIONS

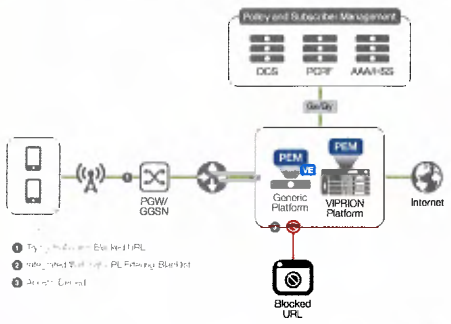
URL Filtering

THE CHALLENGE

The increasing percentage of young children and teenagers using devices to access the Internet can be a cause of concern for many parents, especially as it relates to the inappropriate content that is easily accessible and often unmonitored. Service providers need to come up with solutions that allow parents to control what sites their children can [illegible]. In addition, [illegible] comply with country regulations to block access to blacklisted content and provide a higher QoE for all of their subscribers.

F5 HELPS YOU:

- Increase revenues
- Maximize subscriber QoE



THE SOLUTION

Service providers have an option to integrate URL filtering services within BIG-IP PEM. With URL filtering, you can implement parental control services by blocking traffic to specific websites based on specific URL categories. Parental control services allow you to offer new revenue-generating services that provide greater QoE for subscribers.

In many countries, the service provider is responsible for URL filtering and content blocking to ensure that subscribers do not have access to potentially harmful content and that they adhere to cultural regulations. With built-in blacklisting capabilities, the F5 solution enables you to block access to a set of defined URLs or specific categories, such as gambling or child pornography, and allows access to specific content as defined by whitelists.

DATA TRAFFIC MANAGEMENT SOLUTIONS

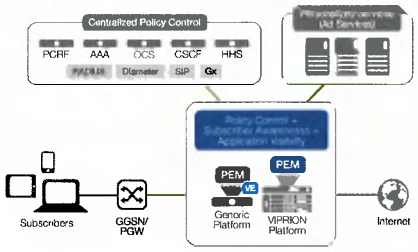
Content Insertion

THE CHALLENGE

Service providers are continuously looking for ways to monetize and increase brand loyalty from subscribers. The devices used by mobile subscribers can provide a wealth of information to service providers including subscriber location, applications used, and content viewed. Service providers can leverage this data to offer personalized services and insert content (such as ads and toolbars) within their devices that [illegible]

F5 HELPS YOU:

- [illegible]
- Increase subscriber brand loyalty

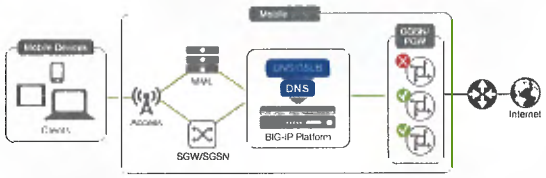


THE SOLUTION

Personalized services offer a better subscriber experience while improving top-line revenue. With the BIG-IP system, you'll gain subscriber and context awareness, and a deep understanding of subscribers' mobile preferences. The BIG-IP system also allows you to insert targeted information into HTTP headers on mobile devices. For example, a subscriber using a mobile device to look for a coffee shop could receive a discount ad for the nearest location. This type of service personalizes the subscriber experience and also opens up additional business/revenue opportunities—with the local retail stores paying you to insert ads into HTTP headers.

SIGNALING SOLUTIONS

Intelligent DNS for the Mobile Core



THE CHALLENGE

Today most operators use a set of Domain Name System (DNS) solutions in the mobile core or Evolved Packet Core (EPC) to provide a [illegible] critical services. DNS provides the directory service by connecting service names to addresses. When a service request is initiated, DNS provides a static list of packet gateways. However, these gateways are not monitored, which makes the list non-deterministic (not based on monitoring or capacity). Overloading of a packet gateway can cause poor performance and service due to dropped connections and unanswered requests.

F5 HELPS YOU

- [illegible]
- Avoid [illegible] dly to required load
- [illegible] overhead through [illegible] routing
- [illegible] quickly to be added or [illegible]

THE SOLUTION

By using F5 DNS and global server load balancing (GSLB) services for infrastructure deployments in the mobile core, the health and status of packet gateways or GGSNs can be monitored. When subscribers need high-speed access to billing, support, and Internet services, you can realize additional value from BIG-IP DNS.

With customizable monitors, you can use the GSLB function to allocate the best resources to DNS queries and respond with the best service experience. For example, the gateway selection process can be optimized by automatically monitoring the packet gateway devices and only providing answers to the DNS queries for gateways that are active and available

BIG-IP DNS adds real-time intelligence to the packet gateway and GGSN selection process, which is critical for service delivery. BIG-IP DNS distributes the load intelligently across available GGSN and packet gateways, ensuring an optimal subscriber experience at all times.

SIGNALING SOLUTIONS

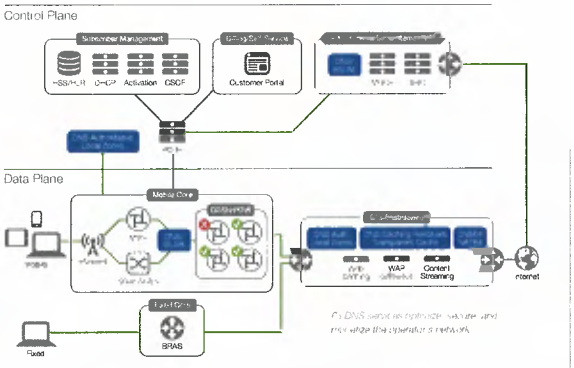
Intelligent DNS Infrastructure

THE CHALLENGE

DNS is a core Internet technology and one of the most important components in a service provider's networking infrastructure, enabling users to access web applications and services. If DNS is unavailable, services will fail to function properly. Service providers need to build an optimized and secure DNS infrastructure to better serve their users. However, creating this infrastructure requires a tremendous amount of real-time management, stability, and room to grow. Scaling DNS rapidly becomes a critical issue when dealing with millions of service names and IP addresses. As service providers scale their control plane, they also need to ensure the security of subscriber and billing data, as well as the capacity to withstand attacks. These include DDoS attacks. DNS-specific [illegible] attacks.

F5 HELPS YOU:

- Optimize network performance
- Maximize subscriber QoE
- Inc[illegible] gence, [illegible] automation



THE SOLUTION

BIG-IP DNS makes it easy for you to optimize, secure, and monetize your DNS infrastructures. It provides carrier-grade, high-performance LDNS caching and resolving, and is a hyperscale authoritative DNS solution that includes security service capabilities. BIG-IP DNS delivers an intelligent and scalable DNS infrastructure for faster access and web response to services for mobile users. In addition, it can load balance local and recursive DNS services. BIG-IP DNS also enables a DNS64 environment, creating a fault-tolerant architecture—optimizing network traffic and increasing QoE.

SIGNALING SOLUTIONS

Interworking—SDC

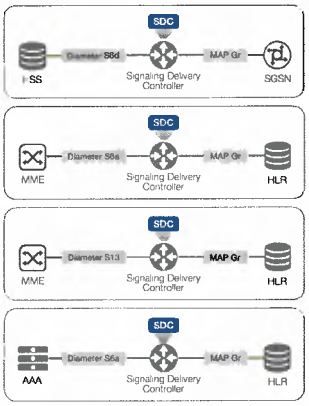
THE CHALLENGE

An interworking function (IWF) acts as a gateway to enable 2G and 3G network elements to connect and communicate with 4G LTE network elements—for instance, between SS7 MAP-based or Diameter-based interfaces. This connection is essential. Without it, service providers would have to totally replace their legacy infrastructure and systems while building out their LTE networks.

When introducing new IMS or LTE elements equipped with Diameter protocol connectivity into the core network, you must ensure that these elements integrate quickly and interface well with the other network elements, regardless of their legacy generation or vendor origin. An IWF ensures that old and new network elements can integrate and connect seamlessly with each other.

F5 HELPS YOU:

- Protect existing infrastructure investments
- Generate new revenue streams



THE SOLUTION

The F5 Traffix Signaling Delivery Controller (SDC) offers interworking functionality through its Diameter gateway to ensure interoperability in a multi-vendor environment. The SDC provides RADIUS-Diameter gateway functionality, allowing RADIUS-based AAAs to communicate via Diameter and Radius-MAP interworking for HLR authentication of WiFi traffic. It also supports legacy protocols and mapping for legacy network connectivity, such as between SS7 and Diameter interfaces. In this way, you can transition easily from legacy to LTE infrastructure. The SDC Diameter gateway enables connectivity between old and new network elements and also supports interconnectivity in roaming.

SIGNALING SOLUTIONS

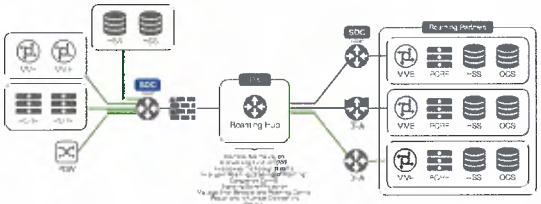
LTE Roaming

THE CHALLENGE

As service providers deploy LTE networks, they need to provide roaming services to LTE subscribers, including connectivity between LTE and 2.5G/3G roamers. This complex process requires addressing routing, scalability, and security issues while maintaining high QoS.

F5 HELPS YOU:

- Achieve faster time to market with new roaming partners
- Introduce new services
- [illegible]



THE SOLUTION

The Traffix SDC helps you fulfill technical requirements and generate revenue from roaming. To overcome the complexity resulting from connecting roamers using different technologies (e.g., 2G/3G versus 4G), the SDC works as an IWF, Diameter gateway, and Diameter Edge Agent (DEA)—providing connectivity, routing, translation capabilities, and extensive security. When deploying the SDC, you can connect quickly and safely with all other mobile networks, wholesale roaming providers, and IP eXchange (IPX) carriers.

SIGNALING SOLUTIONS

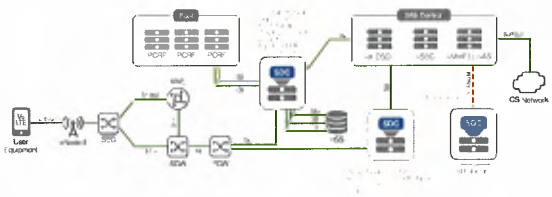
SIP/IMS

THE CHALLENGE

With LTE, service providers are delivering higher broadband speeds, rich multimedia communication services, and VoLTE to achieve service differentiation and increased ARPU. To accomplish this, service providers have implemented IMS architectures, with SIP being one of the primary signaling protocols required to enable innovative applications and services. However, migrating to an all IP-based network has its challenges, including security concerns. Specifically, the connectionless protocols that make IP networks and services prone to attacks that include DoS, DDoS, stealth attacks, and botnets, which can pose considerable SIP requests. In addition, migration to all IP-based networks can pose challenges in managing capacity and performance as subscriber usage continues to increase over time, and, most importantly, in ensuring that all IP-based services are always available.

F5 HELPS YOU:

- Ensure interoperability of SIP requests and responses throughout IP infrastructure
- Scale to handle millions of subscriber calls simultaneously
- Enhance reliability at carrier grade levels, including session synchronization and full failover capabilities with no connection loss



F5 delivers SIP solutions as part of a highly available, scalable, and secure system for the IMS network infrastructure, including devices such as X-CSCF servers and session border controllers (SBC).

THE SOLUTION

The F5 BIG-IP platform delivers SIP solutions as part of a highly available, scalable, and secure system for the IMS network infrastructure, including devices such as X-CSCF servers and session border controllers (SBC).

BIG-IP devices or virtual editions are positioned in front of SIP infrastructure and application servers. Here, they manage SIP traffic and ensure service availability by continuously monitoring the SIP servers and applications at layer 7 and by managing sessions between the different servers. Based on the health and load of the servers, each new SIP session is forwarded to the most appropriate server. In addition, the BIG-IP platform can perform advanced health checks on SIP devices and route SIP clients away from unstable servers, providing increased reliability to existing SIP solutions. BIG-IP instances provide SIP normalization, ensuring there are no interoperability issues between IMS services by transforming the SIP requests and responses as necessary between multiple devices within the IMS architecture.

The BIG-IP platform also enhances security by detecting and automatically dropping SIP communications that are malformed or contain errors. In addition, BIG-IP instances can log and report any unusual increase in SIP requests, including content that is malformed, contains errors, or otherwise appears to rapidly increase the threat of attacks.

NETWORK FUNCTIONS VIRTUALIZATION

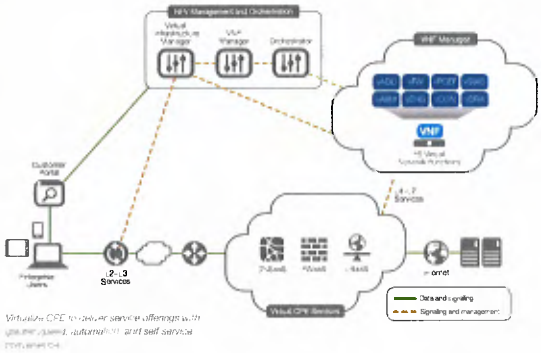
Virtual CPE

THE CHALLENGE

Launching and deploying new services to enterprise customers can significantly challenge service providers. Service providers must often dispatch multiple technicians to install and provision services and customer premises equipment (CPE) in each customer location. In addition, when customers want to change a service or add capacity, the service provider needs to go on-site again to reconfigure, upgrade, or swap out the CPE. From the enterprise perspective, any change requires them to schedule time and wait for the service to be turned on. Slow delivery times can lead to lost business, which in turn can lead to lost revenues for the service provider, as well as lower customer satisfaction.

F5 HELPS YOU:

- Quickly introduce and deploy new network services
- Reduce CapEx and OpEx for delivery of services on customer premises
- Achieve end to end service automation and orchestration
- Quickly and cost-effectively scale services
- Improve customer satisfaction and retention



Virtual CPE to deliver service offerings with greater speed, automation, and self-service provisioning.

THE SOLUTION

Virtual CPE helps service providers take advantage of common network functions virtualization (NFV) infrastructure for services deployed in the cloud and in the network. With NFV, where multiple core network functionalities are offered, virtual CPE enables service providers to adopt a cloud model. This cloud model enables you to share a common pool of resources and dynamically allocate physical compute and network resources to virtual network functions (VNF). You can deploy individual instances of virtualized network functions and offer them as services on customer premises.

Enterprise customers can spin up or spin down instances of network functions or order new services that can be dynamically provisioned in a single location or multiple global locations. Services can be ordered and provisioned via a self-service web portal offered by the service provider. This self-service enables service providers and enterprises alike to move from the complexities, costs, and long delivery cycles associated with deploying physical devices to a cloud-centric, automated, and agile model of service delivery as and wherever needed.

All F5 VNFs can be deployed as a service, including load balancing as a service (LBaaS), firewall as a service (FWaaS), and DNS as a service (DNSaaS). By taking advantage of virtual CPE, you'll achieve faster deployments in the network, faster recognition, higher revenues from service monetization, and a higher return on investment (ROI).

NETWORK FUNCTIONS VIRTUALIZATION

Virtual Gi LAN

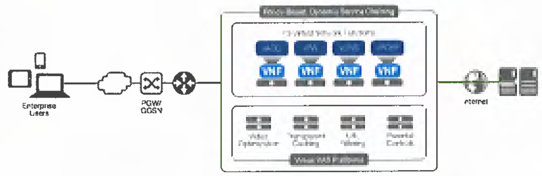
THE CHALLENGE

[illegible] Within the Gi LAN are services including network address translation (NAT), firewall, policy management, traffic steering, and URL filtering, as well as TCP and video optimization. Service providers are able to intelligently steer traffic [illegible] or apply intelligent policy management actions based on subscriber and application awareness.

[illegible] LAN, which in many cases consists of solutions from multiple vendors. For that reason, adding new services to the network can result in increased CapEx and OpEx while introducing additional complexities and increased points of failure into the network. As a result, delivery of new services to subscribers becomes more complex, with major delays, leading to loss of new revenue streams and lowered subscriber QoE.

F5 HELPS YOU:

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]



Simplify the network and speed time to market with a virtual Gi LAN.

THE SOLUTION

A virtualized Gi LAN solution from F5 enables you to build a cost-effective model, allowing for faster time to market for new services while reducing network complexity. F5 VNFs are a core component within an efficient virtual Gi LAN, providing solutions such as virtual policy enforcement, virtual firewall, and virtual Application Delivery Controller (ADC) services. These virtual solutions enable you to provide intelligent traffic steering to VAS components. You can dynamically chain together services based on real-time subscriber and application awareness, as well as secure the Gi LAN. By deploying a common, shared set of commercial, off-the-shelf (COTS) hardware to run various functions—network functions as well as software—you can reduce hardware costs as well as deploy multiple services dynamically. This cloud-like model means you can deliver service functions based on real-time network conditions and improve network resource utilization. You also achieve greater service agility, as you can launch new services without any network downtime. A virtual Gi LAN allows you to innovate, improve subscriber QoE, and lower costs.

NETWORK FUNCTIONS VIRTUALIZATION

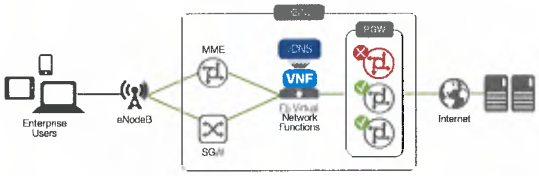
Virtual EPC

THE CHALLENGE

Given increases in mobile data usage, and more notably, exponential growth in video traffic and growing IoT, service providers need to architect their evolved packet cores (EPCs) to not only support the growth in traffic but also to ensure that key [illegible] at all times. As the market evolves, so must the EPC, including the ability to dynamically scale up to meet traffic demands during peak [illegible] and the flexibility to instantiate new services based on real-time network conditions. At the same time, service providers must ensure service availability and meet real-time performance requirements.

F5 HELPS YOU:

- [illegible]
- [illegible]
- [illegible]
- [illegible]



A virtual EPC reduces TCO and enables fast spin-up and spin-down of new services

THE SOLUTION

Virtualizing the EPC allows service providers to quickly realize significant TCO savings and speed time to market for new services. In addition, service providers can reduce OpEx by dynamically spinning up and spinning down various network resources based on network demand and capacity.

F5 solutions using BIG-IP virtual editions include virtualized GTP load balancers, policy management, and Diameter signaling solutions. F5 virtual ADCs—based on BIG-IP® Local Traffic Manager™ (LTM) Virtual Edition—help you perform GTP load balancing among a group of PGWs/SGWs. And by taking advantage of the global server load balancing (GSLB) and dynamic gateway selection functionality of BIG-IP DNS, you can monitor virtual packet gateways and only provide answers to the DNS queries for gateways that are active and available. If a packet gateway goes down, BIG-IP DNS will distribute the traffic load intelligently across only the available packet gateways, ensuring the best subscriber experience.

F5's NFV solutions rely on open REST-based APIs that are interoperable with leading management and orchestration systems, providing a complete NFV ecosystem. These solutions deliver a flexible, agile, and scalable network that helps you deliver services to market faster, improve network efficiency, and reduce CapEx and OpEx.

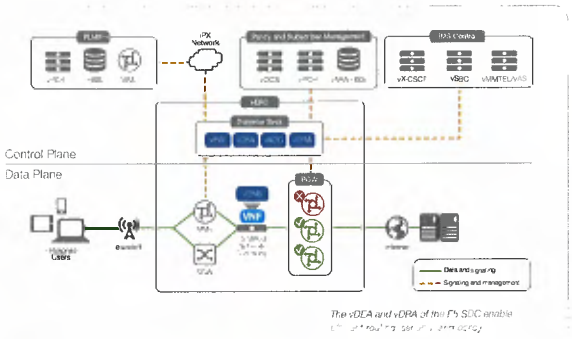
NETWORK FUNCTIONS VIRTUALIZATION

Virtual IMS Network

THE CHALLENGE

Service providers who have deployed LTE networks want to capitalize and monetize the investment, and offering new services such as VoLTE can help open new market opportunities and increase revenue streams. As subscriber growth and demands for network capacity increase, however, service providers also need to build out their networks to rapidly create, launch, and scale new services. A core component of deploying VoLTE services in an LTE network is the IMS network, where SIP and Diameter signaling elements must be scaled out.

F5 HELPS YOU:



The vDEA and vDRA of the F5 SDC enable

THE SOLUTION

Migrating your network to NFV and virtualizing the IMS network will reduce network complexity and costs while providing a scalable solution that enables you to spin up and spin down services based on customer and network requirements.

F5 virtual signaling solutions, including the Traffix SDC, which incorporates the virtual Diameter Routing Agent (vDRA) and virtual Diameter Edge Agent (vDEA), can be deployed to address scaling in network signaling and control planes. With SDC, service providers can ensure delivery of a high QoE for services such as VoLTE running over an IMS network.

The vDRA provides a context-aware routing engine that manages Diameter signaling to ensure high performance and reliability in the control plane. The vDRA also supports LTE network roaming, policy and charging rules, and enforcement, and it interconnects between legacy and LTE network use cases.

The vDEA provides tighter security and normalized functionality in LTE roaming, allowing for IPX carriers to provide security for traffic from other mobile network operators (MNOs) and mobile virtual network operators (MVNOs). The vDEA can also be located at the edge of the network to protect against unexpected signaling surges that can cause service disruption.

F5's virtual ADC (vADC) provides scalability for SIP services within an IMS architecture. The vADC manages SIP traffic and ensures service availability by continuously monitoring SIP servers and applications and managing sessions between the different servers. The vADC also provides SIP security and protects IMS networks from DoS and DDoS attacks, stealth floods, and botnets, as well as malformed or unroutable SIP requests.

CONCLUSION

F5 Solutions for Service Providers

F5 solutions for service providers enable mobile network operators to optimize, secure, and monetize their networks. The solutions use a common, shared platform to reduce operational overhead and improve service-provisioning velocity while addressing key security concerns across the network.

F5 solutions for service providers enable mobile network operators to scale in three dimensions—the control, data, and application planes—supporting the highest [illegible] rates and concurrency levels in the industry.

Control Plane

The control plane is the heart of a service provider network. Tasked with the responsibility for managing subscriber use and ensuring the appropriate services [illegible] by signaling storms that occur due to spikes in activations or, for example, an Internet-wide gaming addiction that causes millions of concurrent players to join in.

The control plane is driven predominantly by Diameter [illegible] SDC, which help mobile network operators scale the control plane while enabling the creation of new [illegible] plane services. This enables service providers to deliver secure, SLA-based services to users.

Data Plane

The service provider data plane serves as the backbone between the mobile network and the Internet, and it must be able to support millions of consumer requests for applications. Bandwidth-hungry applications like video can become problematic for the data plane and cause degradations in performance that hamper the subscriber experience and send subscribers off looking for a new provider.

F5 solutions for service providers include a high-performance services fabric composed of any combination of hardware or virtual network functions (VNFs). F5 VIPRION offerings support up to 1.2 billion concurrent connections and greater than one terabit (1 TBI of throughput, while F5 VNFs and BIG-IP virtual editions (VEs) support L4 throughput up to 70 Gbps. The F5 high-performance services fabric is built on a common, shared, and optimized platform on which key service provider functions can be consolidated. By consolidating services in the Gi network on a single platform, providers can eliminate the operational overhead incurred by the need to manage multiple [illegible] firewalls.

Application Plane

Value-added services are a key differentiator and key revenue opportunity for service providers, but can also be the source of poor performance due to the [illegible] regardless of their applicability. Sending text through a video optimization service or video through an ad insertion service does not add value, but it does consume resources and time—impacting the overall subscriber experience.

F5 solutions for service providers work with virtual machine provisioning systems to help service providers move toward network functions virtualization (NFV) based architectures. Intelligent monitoring of value-added services, combined with awareness of load and demand, enable service providers to ensure that VAS platforms can be scaled up and down individually, [illegible] the VAS infrastructure.

With F5 solutions, mobile network operators can simplify their Gi networks and combine physical [illegible] elastic, high-performance services fabric. This enables [illegible] foundation for rapid service creation and deployment.

F5 enables [illegible] next-generation networks that provide a superior customer experience. Intelligent L4–L7 network devices play a primary role in the F5 approach to solution design, allowing service providers to maintain high network performance while expanding customized products and [illegible]

Diameter Signaling Management

Diameter signaling messages serve as an excellent source of information on network operations and subscribers. When extrapolated, this information may be used to differentiate service offerings and improve the customer experience. As the market's most mature Diameter solution, the SDC consolidates a Diameter Routing Agent (DRA), a Diameter Edge Agent (DEA), a Diameter load balancer, and a Diameter gateway and translation (including IWF) on a single [illegible] subscriber- and [illegible] aware intelligent routing, reliable load balancing, and [illegible] connectivity.

Intelligent Traffic Management and Policy Enforcement

[illegible] services such as dynamic service chaining. Using control- and subscriber-aware technology, BIG-IP PEM offers a full-proxy architecture and rich IP capabilities [illegible] the ability to inspect and [illegible] traffic based on data [illegible]

DNS Services to Manage Network Growth

F5's comprehensive control and data plane solutions optimize, intelligently scale, and securely manage messaging interfaces such as RADIUS, DNS, and SIP. The F5 DNS solution, BIG-IP DNS, allows service providers to optimize their LDNS, authoritative DNS, and infrastructure DNS—delivering a high subscriber QoE that results in increased revenues and reduced churn.

Carrier-Grade Network Firewall Security

F5 provides integrated, high-performance ICSA [illegible] infrastructure and scale to perform under the most [illegible] increasingly threatening landscape—with a common platform to deliver applications and improve responsiveness. BIG-IP® Application Security Manager™ (ASM) enhances security for applications by providing comprehensive web security and L7 DDoS protection.

SDN and NFV Solutions

With F5 solutions, service providers can move to [illegible] architectures for greater agility. They can deploy applications and services across multiple hybrid network architectures and evolving NFV environments using both F5's purpose-built, carrier-grade chassis and VNFs. The fully virtualized, carrier-grade F5 network [illegible] agile network. Operators can rapidly test and deliver a variety of personalized services while managing rapid [illegible]

F5 solutions also help generate new revenues through services such as parental controls, enhanced security, shared data plans, application-based charging, VoLTE, URL filtering, [illegible] operators take advantage of new opportunities to grow new revenue streams.

About F5

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, and SDN deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

GUIDE-SP-CONF-66589956 | 0216